



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto  
is a true copy from the records of the Korean Intellectual  
Property Office.

출원 번호 : 10-2003-0010412  
Application Number

출원 년 월 일 : 2003년 02월 19일  
Date of Application FEB 19, 2003

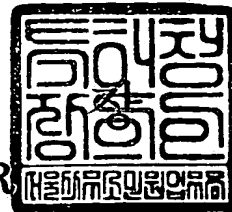
출원인 : 삼성전자주식회사  
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003      년      09      월      17      일

특      허      청

COMMISSIONER



## 【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0009
【제출일자】	2003.02.19
【국제특허분류】	H04L
【발명의 명칭】	모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법
【발명의 영문명칭】	Router for providing linkage with mobile node, and the method thereof
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2003-003435-0
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2003-003436-7
【발명자】	
【성명의 국문표기】	이학구
【성명의 영문표기】	LEE, Hak Goo
【주민등록번호】	740418-1457212
【우편번호】	442-743
【주소】	경기도 수원시 팔달구 매탄3동 임광아파트 4동 208호
【국적】	KR
【발명자】	
【성명의 국문표기】	문경환
【성명의 영문표기】	MOON, Kyoung Hwan
【주민등록번호】	751029-1357114

**【우편번호】** 442-804  
**【주소】** 경기도 수원시 팔달구 매탄3동 871-11 B05호  
**【국적】** KR  
**【발명자】**  
**【성명의 국문표기】** 김평수  
**【성명의 영문표기】** KIM,Pyung Soo  
**【주민등록번호】** 720205-1222719  
**【우편번호】** 137-892  
**【주소】** 서울특별시 서초구 양재동 160-2번지 양재우성아파트 113동 406호  
**【국적】** KR  
**【심사청구】** 청구  
**【취지】** 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인  
 이영필 (인) 대리인  
 이해영 (인)  
**【수수료】**  
**【기본출원료】** 20 면 29,000 원  
**【가산출원료】** 17 면 17,000 원  
**【우선권주장료】** 0 건 0 원  
**【심사청구료】** 11 항 461,000 원  
**【합계】** 507,000 원  
**【첨부서류】** 1. 요약서·명세서(도면)\_1통

**【요약서】****【요약】**

모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법이 개시된다. 본 발명에 따른 라우터는, 모바일 노드와의 통신을 위해 필요한 모바일 기능을 구비하지 아니한 상대방 노드를 대신하여 보안을 위한 인증 과정, 바인딩 업데이트 과정 및 패킷 변환 과정 등을 수행하여 모바일 노드와 상대방 노드간에 패킷을 교환한다. 본 발명에 따른 모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법은, 모바일 노드와의 통신을 위해 필요한 모바일 기능을 구비하지 아니한 상대방 노드와 모바일 노드간의 직접 통신을 가능하게 하는 효과를 제공한다.

**【대표도】**

도 4

## 【명세서】

## 【발명의 명칭】

모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법{Router for providing linkage with mobile node, and the method thereof}

## 【도면의 간단한 설명】

도 1은 모바일 노드와 상대방 노드간의 접속을 제공하는 본 발명에 따른 라우터가 적용된 시스템을 나타내는 도면,

도 2는 홈 에이전트의 바인딩 정보를 업데이트하는 과정을 설명하기 위한 흐름도,

도 3은 인캡슐레이션과 디캡슐레이션을 설명하기 위한 도면,

도 4는 본 발명에 따른 라우터의 상세 구성을 설명하기 위한 도면,

도 5는 본 발명에 따른 라우터에 의해 수행되는 보안을 위한 인증 과정을 설명하기 위한 도면,

도 6은 모바일 노드가 두 개의 인증요청패킷을 송신한 경우를 나타내는 도면,

도 7은 인증 테이블의 일 예를 나타내는 도면,

도 8은 본 발명에 따른 라우터에서의 바인딩 업데이트 과정을 설명하기 위한 흐름도,

도 9는 바인딩 캐쉬의 일 예를 나타내는 도면,

도 10은 바인딩 업데이트 후, 모바일 노드가 상대방 노드로 전송한 패킷을 라우터가 처리하는 과정을 설명하기 위한 흐름도,

도 11은 데이터 저장부내의 네이버 캐쉬의 일 예를 나타내는 도면,

도 12는 패킷 변환부가 패킷의 소스 어드레스를 변환하는 일 예를 나타내는 도면,

도 13은 상대방 노드가 전송한 패킷을 수신하여 처리하는 과정을 설명하기 위한 흐름도,  
도 14는 패킷 변환부가 패킷의 목적지 어드레스를 변환하는 일 예를 나타내는 도면이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

- <15> 본 발명은 모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법에 관한 것으로서, 보다 상세하게는 모바일 노드와의 통신을 위한 모바일 통신 기능을 구비하지 아니한 상대방 노드와 모바일 노드간의 통신을 가능하게 하는 라우터 및 그 라우팅 방법에 관한 것이다.
- <16> 종래에 사용된 인터넷 프로토콜 버전 4(Internet Protocol Version 4, 이하 IPv4라 함)를 개선하기 위해 인터넷 프로토콜 버전 6(Internet Protocol Version 6, 이하 IPv6라 함)가 개발되고 있다. IPv6는 차세대 IP(IP Next Generation)라고도 불린다.
- <17> IPv6의 가장 큰 특징은 IP주소의 길이가 32 비트에서 128 비트로 늘어났다는 점이다. 인터넷이 폭발적으로 성장함에 따라 네트워크 주소가 고갈될 것에 대비하여 IP주소 길이를 확장하였다.
- <18> IPv6는 헤더 영역이 확장됨으로서 패킷의 출처 인증, 데이터 무결성의 보장 및 비밀의 보장 등을 위한 메커니즘을 지정할 수 있도록 하고 있다.
- <19> 한편, 휴대용 컴퓨터와 같은 모바일 노드(Mobile Node)가 IPv6를 통해 통신하는 기능을 제공하는 모바일 IPv6가 개발되어왔다.

- <20>        모바일 IPv6는 홈 링크 영역에서 부여받은 홈 어드레스를 가지고 있는 모바일 노드가 홈 링크 영역을 떠나 원격지 링크 영역으로 이동한 경우에도, 원격지 링크 영역에서 부여받은 원격지 주소(Care of Address:CoA)를 이용하여 통신하고자 하는 상대방 노드(Correspondent Node)와 통신할 수 있게 한다.
- <21>        모바일 IPv6에 관한 보다 상세한 내용은 IETF (Internet Engineering Task Force)에서 작성한 "Mobility Support in IPv6"(draft-ietf-mobileip-ipv6-20.txt)에 기재되어 있다.
- <22>        그러나, 모바일 IPv6 기능을 구비한 모바일 노드가 상대방 노드와 통신을 할 수 있기 위해서는 상대방 노드 또한 모바일 IPv6 기능을 구비하여야 하는 문제가 있다.
- <23>        보다 상세하게 설명하면, 모바일 IPv6에서는 모바일 노드와 상대방 노드사이에 보안에 관련된 인증을 수행한 후, 양자간에 바인딩(binding) 과정을 거치게된다. 이후에는 모바일 노드의 원격지 주소(CoA)를 이용하여 모바일 노드의 홈 링크의 홈 에이전트를 거치지 않고, 양자간의 직접 통신이 가능하게 된다. 따라서 상대방 노드는 보안에 관한 인증과정과 바인딩 과정에 필요한 기능을 구비하여야 한다. 그러나 모바일 IPv6가 아닌 일반적인 IPv6 프로토콜에는 이와 같은 기능을 수행할 수 없다.
- <24>        또한 모든 상대방 노드들에게 모바일 IPv6의 기능을 부여하기까지는 많은 시간 및 비용이 소요되는 문제가 있다.

**【발명이 이루고자 하는 기술적 과제】**

- <25>        따라서 본 발명이 이루고자 하는 기술적 과제는, 모바일 노드와의 통신을 위한 모바일 기능을 구비하지 아니한 상대방 노드와 모바일 기능을 구비한 모바일 노드간의 통신을 가능하게 하는 라우터 및 그 라우팅 방법을 제공하는데 있다.

## 【발명의 구성 및 작용】

- <26>       상기 과제를 이루기 위해, 본 발명에 의한 라우터는,
- <27>       원격지 링크에 접속한 모바일 노드와 상대방 노드간에 패킷을 전달하는 라우터에 있어서, 적어도 인증키 생성 토큰을 생성하기 위한 데이터를 저장하는 데이터 저장부; 패킷을 수신하거나 송신할 패킷의 헤더에 기록된 목적지 어드레스로 패킷을 송신하는 제1 인터페이스; 상기 제1 인터페이스로부터의 출력된 패킷이 상기 모바일 노드의 인증을 요청하는 인증요청패킷이면 상기 인증요청패킷을 출력하는 패킷 감시부; 상기 패킷 감시부의 출력인 상기 입력 패킷을 입력받아, 상기 데이터 저장부에 저장된 인증키 생성 토큰을 생성하기 위한 데이터를 참조하여 인증키 생성 토큰을 생성하고, 상기 인증키 생성 토큰을 이용하여 인증키를 생성한 후, 상기 인증키 생성 토큰 및 상기 인증키를 상기 데이터 저장부에 저장하고, 상기 인증키 생성 토큰을 상기 제1 인터페이스로 출력하는 제어부를 포함하고, 상기 제1 인터페이스는 상기 인증키 생성 토큰을 입력받아 상기 모바일 노드로 전송한다.
- <28>       또한, 상기 패킷 감시부는 상기 제1 인터페이스가 수신하여 출력한 패킷이 상기 모바일 노드가 상기 인증키 생성 토큰에 따라 생성한 인증키를 이용하여 암호화한 바인딩 업데이트 패킷이면 상기 바인딩 업데이트 패킷을 상기 제어부로 출력하고, 상기 제어부는 상기 바인딩 업데이트 패킷에 포함된, 상기 모바일 노드의 홈 어드레스와 상기 원격지 링크에서 부여받은 원격지 어드레스를 포함하는 바인딩 정보를 상기 데이터 저장부에 저장된 상기 인증키를 이용하여 추출하여 상기 데이터 저장부에 저장하는 것이 바람직하다.
- <29>       또한 상기 라우터는 상기 패킷 감시부로부터 출력된 패킷을 입력받아, 상기 제어부의 제어에 따라 상기 모바일 단말기의 원격지 주소로 설정된 소스 어드레스를 상기 홈 어드레스로 패킷을 변환하여 출력하는 패킷 변환부; 및 상기 패킷 변환부에서 출력된 패킷을 입력받아, 상



기 패킷의 헤더에 기록된 상기 상대방 노드의 어드레스에 따라 상기 패킷을 상기 상대방 노드로 전송하는 제2 인터페이스를 더 포함하고, 상기 패킷 감시부는 상기 제1 인터페이스가 수신하여 출력한 패킷의 헤더를 검색하여, 상기 패킷 헤더에 포함된 바인딩 정보를 상기 제어부로 출력하고, 상기 패킷 변환부로 수신한 패킷을 출력하고, 상기 제어부는 상기 데이터 저장부를 검색하여 상기 바인딩 정보가 상기 데이터 저장부에 존재하면, 소스 어드레스가 상기 홈 어드레스로 변환된 패킷을 출력하도록 상기 패킷 변환부를 제어한다.

<30> 또한, 상기 제어부는 상기 데이터 저장부를 검색하여 상기 바인딩 정보가 상기 데이터 저장부에 존재하지 않으면, 상기 패킷에 포함된 소스 어드레스를 변환하지 않고 상기 패킷을 통과시키도록 상기 패킷 변환부를 제어한다.

<31> 또한, 상기 제2 인터페이스는 상기 상대방 노드가 송신한 패킷을 수신하여 상기 패킷 감시부로 출력하고, 상기 패킷 감시부는, 상기 제2 인터페이스로부터 입력받은 패킷의 헤더에 기록된 목적지 어드레스를 상기 제어부로 출력하고, 상기 패킷 변환부로 입력받은 패킷을 출력하고, 상기 제어부는 상기 데이터 저장부를 검색하여 상기 목적지 어드레스가 상기 모바일 노드의 홈 어드레스이고 상기 홈 어드레스가 상기 모바일 노드의 원격지 어드레스와 바인딩되어 있으면, 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하도록 상기 패킷 변환부를 제어하고, 상기 패킷 변환부는 상기 제어부의 제어에 따라 상기 상대방 노드가 송신한 패킷의 헤더에 기록된 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하여 상기 제1 인터페이스로 출력한다.

<32> 상기 과제를 이루기 위해, 본 발명에 의한 라우팅 방법은,

<33> 원격지 링크에 접속한 모바일 노드와 상대방 노드간에 패킷을 전달하는 라우팅 방법에 있어서, (a) 상기 모바일 노드로부터 송신된 패킷이 상기 모바일 노드의 인증을 요청하는 인증

요청패킷인지 여부를 감시하는 단계; (b) 상기 모바일 노드로부터 송신된 패킷이 상기 모바일 노드의 인증을 요청하는 인증요청패킷이면, 미리 저장된 인증키 생성 토큰을 생성하기 위한 데이터를 참조하여 인증키 생성 토큰을 생성하는 단계; (c) 생성된 인증키 생성 토큰에 따라 생성한 인증키 및 상기 인증키 생성 토큰을 저장하는 단계; 및 (d) 상기 모바일 노드로 상기 인증키 생성 토큰을 송신하는 단계를 포함한다.

<34> 또한, 상기 라우팅 방법은, (e) 상기 모바일 노드가 상기 인증키 생성 토큰에 따라 생성한 인증키를 이용하여 인증한 바인딩 업데이트 패킷을 수신하는 단계; 및 (f) 상기 바인딩 업데이트 패킷에 포함된, 상기 모바일 노드의 홈 어드레스와 상기 원격지 링크에서 부여받은 원격지 어드레스를 포함하는 바인딩 정보를 미리 저장한 상기 인증키를 이용하여 추출한 후 저장하는 단계를 더 포함하는 것이 바람직하다.

<35> 또한, 상기 라우팅 방법은, (g) 상기 모바일 노드가 송신한 패킷으로서 바인딩 정보 및 데이터를 포함하는 패킷을 수신하는 단계; (h) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하는지 여부를 검색하는 단계; (i) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하면, 상기 원격지 주소로 설정된 소스 어드레스를 상기 홈 어드레스로 변환하는 단계; 및 (j) 상기 소스 어드레스가 변환된 패킷을 상기 상대방 노드로 전송하는 단계를 더 포함한다.

<36> 또한, 상기 라우팅 방법은, (k) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하지 않으면, 상기 패킷에 포함된 소스 어드레스를 변환하지 않고 패킷을 상기 상대방 노드로 전송하는 단계를 더 포함한다.

- <37> 또한, 상기 라우팅 방법은, (l) 상기 상대방 노드가 송신한 패킷의 헤더에 목적지 어드레스로 기록된 상기 모바일 노드의 홈 어드레스를 추출하는 단계; (m) 저장된 다수의 바인딩 정보를 검색하여 상기 모바일 노드의 홈 어드레스와 바인딩된 상기 모바일 노드의 원격지 어드레스를 추출하는 단계; (n) 상기 상대방 노드가 송신한 패킷의 헤더의 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하는 단계; 및 (o) 상기 상대방 노드의 원격지 어드레스에 따라 상기 상대방 노드가 송신한 패킷을 상기 모바일 노드로 송신하는 단계를 더 포함한다.
- <38> 이하, 첨부된 도면들을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명한다.
- <39> 도 1은 모바일 노드(10)와 상대방 노드(60~80)간의 접속을 제공하는 본 발명에 따른 라우터(100)의 적용도이다.
- <40> 모바일 노드(10)는 모바일 IPv6기능을 구비한 휴대용 장치이다. 모바일 노드(10)는 예컨대 휴대용 컴퓨터 및 PDA(Personal Digital Assistant) 등으로 구현된다.
- <41> 홈 에이전트(30)는 홈 링크(20) 영역 내에 위치한 라우터로서, 모바일 노드(10)의 홈 어드레스가 등록된 라우터이다.
- <42> 상대방 노드인 CN1(60), CN2(70) 및 CN3(80)는 모바일 IPv6기능을 구비하지 아니하고 일반적인 IPv6기능을 구비한 노드들이다. 상대방 노드들은 모바일 노드이던 비모바일 노드이든 무방하다. 상대방 노드는 예컨대, FTP(File Transfer Protocol) 서버, HTTP(Hyper Text Transfer Protocol) 서버 및 SMTP(Simple Mail Transfer Protocol) 서버 등이다.
- <43> 홈 링크(20) 영역 내에 위치하던 모바일 노드(10)가 원격지 링크(40)로 이동하면, 본 발명에 따른 라우터(100)를 통해 모바일 노드(10)가 상대방 노드들(60~80) 중의 하나와 통신을

하기 위해서는 홈 에이전트(30)에 모바일 노드(10)의 홈 어드레스와 원격지 어드레스(CoA)를 바인딩한 바인딩 정보를 업데이트시켜야 한다.

<44> 도 2는 홈 에이전트(30)의 바인딩 정보를 업데이트하는 과정을 설명하기 위한 흐름도이다.

<45> 도 1 및 도 2를 참조하여 홈 에이전트(30)의 바인딩 정보를 업데이트하는 과정을 설명한다.

<46> 홈 링크(20) 영역 내에 위치하던 모바일 노드(10)가 모바일 노드(10)의 사용자에 의해 원격지 링크(Foreign Link)(40)로 이동한다(제210 단계).

<47> 원격지 에이전트(50)(Foreign Agent)는 모바일 노드(10)가 원격지 링크(40)로 들어온 것을 감지하여 모바일 노드(10)에게 원격지 어드레스(CoA)를 부여한다(제230 단계).

<48> 원격지 어드레스(CoA)를 부여받은 모바일 노드(10)는 바인딩 업데이트 메시지를 홈 에이전트(30)에게 전송한다(제250 단계). 바인딩 업데이트 메시지에는 소스 어드레스가 원격지 어드레스(CoA)이고 목적지 어드레스(Destination Address)가 홈 에이전트(30)의 어드레스인 헤더가 포함되어 있다.

<49> 모바일 노드(10)의 원격지 어드레스(CoA)를 포함한 바인딩 업데이트 메시지를 수신한 홈 에이전트(30)는 모바일 노드(10)의 홈 어드레스와 원격지 어드레스(CoA)를 바인딩하여 저장한다(제270 단계). 따라서 모바일 노드(10)가 원격지 링크로 이동하더라도, 상대방 노드가 송신한 패킷을 홈 에이전트(30)는 저장된 바인딩 정보를 참고하여 원격지의 모바일 노드(10)로 패킷을 전달할 수 있다.

- <50> 홈 에이전트(30)에 모바일 노드(10)의 바인딩 정보가 업데이트된 후, 상대방 노드들 (60~80) 중의 하나, 예컨대 CN1(60)이 모바일 노드(10)로 최초로 패킷을 전송한다. CN1(60)은 모바일 노드(10)의 홈 어드레스만을 알고 있으므로 CN1(60)이 전송한 패킷의 헤더에 기록된 목적지 어드레스는 모바일 노드(10)의 홈 어드레스이다. 홈 에이전트(30)는 CN1(60)이 송신한 패킷을 수신하면 바인딩 업데이트 과정에 의해 미리 저장된 모바일 노드(10)의 바인딩 정보를 참고하여 인캡슐레이션(encapsulation)을 수행하여 원격지 링크에 위치한 모바일 노드(10)로 패킷을 전송한다.
- <51> 도 3은 홈 에이전트(30)에 의한 인캡슐레이션과 모바일 노드(10)에 의한 디캡슐레이션(decapsulation)을 설명하기 위한 도면이다.
- <52> CN1(60)이 모바일 노드(10)의 홈 어드레스를 목적지 어드레스로 하여 송신한 패킷을 홈 에이전트(30)가 수신하면, 홈 에이전트(30)는 바인딩 정보를 검색하여 모바일 노드(10)의 원격지 어드레스를 검색한다. 홈 에이전트(30)는 도 3에 도시한 바와 같이 검색된 원격지 어드레스를 수신한 패킷에 추가하는 인캡슐레이션(encapsulation)하여 원격지의 모바일 노드(10)에게 전송한다.
- <53> 인캡슐레이션된 패킷을 수신한 원격지의 모바일 노드(10)는 다시 수신한 패킷을 도 3에 도시한 바와 같이 디캡슐레이션함으로써 CN1(60)이 모바일 노드(10)에게 송신한 원래 패킷을 상위 계층으로 전달할 수 있게된다.
- <54> CN1(60)이 송신한 패킷을 홈 에이전트(30)로부터 전송받은 모바일 노드(10)는 라우터 (100)와의 보안을 위한 인증 과정 및 바인딩 업데이트 과정을 수행한 후 실제 데이터를 라우터 (100)를 통해 CN1(60)으로 전송한다.

- <55> 이하에서는 도면을 참조하여 모바일 노드(10)와 상대방 노드인 CN1(60)과의 통신을 위해, 모바일 노드(10)와 인증 과정 및 바인딩 업데이트 과정을 수행한 후 실제 데이터를 모바일 노드(10)와 CN1(60)사이에 전달하는 라우터(100)의 동작을 설명한다.
- <56> 도 4는 본 발명에 따른 라우터(100)의 상세구성을 설명하기 위한 도면이다.
- <57> 도 4를 참조하면, 라우터(100)는 제1 인터페이스(110), 패킷 감시부(120), 제어부(130), 데이터 저장부(140), 패킷 변환부(150), 제2 인터페이스(160) 및 관리자 인터페이스(170)를 포함한다.
- <58> 제1 인터페이스(110)는 모바일 IPv6 네트워크(도시되지 않음)를 통해 홈 에이전트(30) 또는 모바일 노드(10)가 송신한 패킷을 수신하거나 홈 에이전트(30) 또는 모바일 노드(10)로 패킷을 송신한다.
- <59> 제2 인터페이스(160)는 CN1(60)이 송신한 패킷을 수신하거나 CN1(60)으로 패킷을 송신한다.
- <60> 패킷 감시부(120)는 제1 인터페이스(110)를 통해 수신한 홈 에이전트(30) 또는 모바일 노드(10)가 송신한 패킷 또는 제2 인터페이스(160)를 통해 수신한 CN1(60)이 송신한 패킷을 감시하여 수신된 패킷의 종류에 따라 제어부(130)로 소정 정보를 전달하거나 제어부(130)의 제어에 따라 수신한 패킷을 패킷 변환부(150)로 전달한다.
- <61> 제어부(130)는 패킷 감시부(120)로부터 패킷 또는 소정 정보를 입력받은 경우, 데이터 저장부(140)에 저장된 데이터를 참조하여 패킷 감시부(120) 및 패킷 변환부(150)를 제어함으로써 본 발명에 따른 인증 과정, 바인딩 업데이트 과정 및 데이터 전달 동작을 제어한다.

- <62> 데이터 저장부(140)는 바인딩 캐시(141), 인증 테이블(143) 및 네이버 캐시(neighbor cashe)(145)를 포함하여, 각각 바인딩 업데이트 정보, 보안을 위한 인증에 관련된 데이터 및 라우터(100)에 접속된 상대방 노드들(60~80)의 IP 어드레스를 저장한다.
- <63> 패킷 변환부(150)는 제어부(130)의 제어에 따라 패킷 감시부(120)로부터 입력받은 패킷의 헤더에 기록된 소스 어드레스 또는 목적지 어드레스를 변환하여, 변환된 패킷을 출력한다.
- <64> 관리자는 관리자 인터페이스(170)를 통해 모바일 IPv6 기능을 구비하지 아니한 상대방 노드들을 대신하여 라우터(100)가 모바일 IPv6 기능을 수행할 상대방 노드들의 IP 어드레스를 입력한다. 제어부(130)는 관리자 인터페이스(170)를 통해 라우터(100)가 모바일 IPv6 기능을 대신하여 수행할 상대방 노드들의 IP 어드레스가 입력되면, 데이터 저장부(140)의 바인딩 캐시(141) 및 인증 테이블(143)에 각 상대방 노드들에 대응하는 데이터 저장 영역을 할당한다.
- <65> 도 5는 라우터(100)에 의해 수행되는 보안을 위한 인증 과정을 설명하기 위한 도면이다.
- <66> 이하에서는 도 4 및 도 5를 참조하여 라우터(100)에 의해 수행되는 보안을 위한 인증 과정을 설명한다.
- <67> 전술한 바와 같이, 모바일 노드(10)는 원격지 링크(40)로 이동하여 원격지 에이전트(50)로부터 원격지 주소를 할당받아 홈 에이전트(30)의 바인딩 정보를 업데이트한 후, CN1(60)이 전송한 최초 패킷을 홈 에이전트(30)로부터 전달받은 모바일 노드(10)이다.
- <68> 모바일 노드(10)는 CN1(60)이 전송한 최초 패킷을 홈 에이전트(30)로부터 전달받아 목적지 어드레스를 CN1(60)의 어드레스로 한 인증요청패킷을 송신한다. 송신된 인증요청패킷을 라우터(100)가 수신한다(제310 단계). 본 실시예에서 표준작업 진행중이 모바일 IPv6에서 규정한 바와 같이, 모바일 노드(10)는 두 개의 인증요청패킷을 생성하여 전송한다.

- <69> 도 6은 모바일 노드(10)가 두 개의 인증요청패킷을 송신한 경우를 나타내는 도면이다.
- <70> 도 6을 참조하면, 모바일 노드(10)는 HoTI(Home Test Init) 및 CoTI(Care-of Test Init)의 두 개의 인증요청패킷을 생성하여 전송한다. HoTI는 홈 에이전트(30)를 거쳐 라우터(100)로 송신되고 CoTI는 직접 라우터(100)로 송신된다.
- <71> HoTI와 CoTI는 라우터(100)의 제1 인터페이스(110)를 통해 패킷 감시부(120)로 입력된다.
- <72> 패킷 감시부(120)는 입력된 패킷이 인증요청패킷인지 여부를 판단한다(제320 단계).
- <73> 패킷 감시부(120)는 입력된 패킷이 인증요청패킷으로 판단되면 제어부(130)로 입력된 패킷을 출력한다. 제어부(130)는 데이터 저장부(140)의 인증 테이블(143)내의 다수의 상대방 노드들에 관한 인증 테이블 중, CN1(60)의 인증 테이블(143a)을 검색한다. 제어부(130)는 CN1(60)의 인증 테이블(143a)내에 저장된 다수의 모바일 노드에 관한 데이터 중, 모바일 노드(10)에 관련된 인증을 위한 데이터인 NONCE 및 Kcn을 읽어들인다. NONCE는 인증키 생성 토큰인 Home Keygen Token 과 Care-of Keygen Token의 생성에 사용되는 난수(random number)로서 난수 발생기(도시되지 않음)에 의해 주기적으로 생성되어 CN1(60)의 인증 테이블(143a)에 저장된다. Kcn 또한 인증키 생성 토큰인 Home Keygen Token 과 Care-of Keygen Token의 생성에 사용되는 값이다.
- <74> 제어부(130)는 NONCE 및 Kcn과 HoTI 및 CoTI에 포함되어 전달된 모바일 노드(10)의 홈 어드레스 및 원격지 어드레스를 이용하여 인증키 생성 토큰인 Home Keygen Token 과 Care-of Keygen Token을 아래의 수학적식에 의해 생성한다(330 단계).
- <75> 【수학적식 1】  $Home\ Keygen\ Token =$



<76> First(64, HMAC\_SHA1(Kcn, (home address|nonce|0)))

<77> 【수학식 2】 Care-of Keygen Token =

<78> First(64, HMAC\_SHA1(Kcn, (care-of address|nonce|1)))

<79> 상기 수학식 1 및 2에 사용된 HMAC\_SHA1 함수는 일종의 해쉬(Hash) 함수이다. First(64, HMAC\_SHA1) 함수는 HMAC\_SHA1 함수에 의해 생성된 비트 중, 처음 64 비트를 출력값으로 한다.

<80> 제어부(130)는 인증키 생성 토큰인 Home Keygen Token 과 Care-of Keygen Token을 생성한 후, 상기 인증키 생성 토큰들을 이용하여 아래의 수학식에 따라 인증키 Kbm을 생성한다(제340 단계).

<81> 【수학식 3】 
$$Kbm = SHA1(Home\ Keygen\ Token | Care-of\ Keygen\ Token)$$

<82> 인증키 생성 토큰인 Home Keygen Token 과 Care-of Keygen Token 및 인증키 Kbm을 생성하는 방법에 관한 보다 상세한 설명은 전술한 모바일 IPv6에 관하여 IETF(Internet Engineering Task Force)에서 작성한 "Mobility Support in IPv6" (draft-ietf-mobileip-ipv6-20.txt)에 기재되어 있다.

<83> 제어부(130)는 생성한 인증키 Kbm과 인증키 생성 토큰을 데이터 저장부(140)의 인증 테이블(143)에 저장한다(제350 단계).

<84> 도 7은 인증 테이블(143)의 일 예를 나타내는 도면이다. 인증 테이블(143)은 각각의 상대방 노드별 인증테이블(143a, 143b)을 구비하고, 각 상대방 노드별 인증테이블은 각 상대방 노드와 통신을 하는 다수의 모바일 노드에 관한 인증을 위한 데이터를 저장한다. 본 실시예에 따른 모바일 노드(10)는 143a에 도시된 MN1이라 가정한다. 모바일 노드(10)의 인증을 위해 생

성된 인증키 Kbm은, 인증키 생성 토큰을 위해 미리 생성되어 저장되어 있던 NONCE, NONCE INDEX 및 Kcn과 함께 저장된다.

- <85> 제어부(130)는 모바일 노드(10)로 수신한 HoTI와 CoTI에 각각 응답하는 HoT(Home Test)와 CoT(Care-of Test)메시지를 송신한다(제360 단계). 도 6에 도시한 바와 같이, HoT 메시지는 홈 에이전트(30)를 거쳐 모바일 노드(10)로 전송되고, CoT 메시지는 직접 모바일 노드(10)로 전송된다. HoT 메시지와 CoT 메시지의 헤더의 소스 어드레스는 라우터(100)의 어드레스가 아닌 모바일 노드(10)가 직접 통신을 원하는 상대방 노드인 MN1(60)의 IP 어드레스이다.
- <86> HoT 메시지와 CoT 메시지는 각각 Home Keygen Token 및 Care-of Keygen Token을 포함하고, NONCE INDEX를 공통으로 포함한다. NONCE INDEX는 Home Keygen Token 및 Care-of Keygen Token의 생성에 사용된 NONCE가 무엇인지를 나타내는 인덱스이다. NONCE INDEX를 송신함으로써 NONCE 그 자체를 송신할 필요가 없다. 라우터(100)는 HoT 메시지와 CoT 메시지를 성공적으로 모바일 노드(10)로 전송함으로써 모바일 노드(10)의 홈 어드레스와 원격지 주소(CoA)의 두 가지 주소로 모두 모바일 노드(10)와 통신 가능함을 확인하게 된다.
- <87> 도 8은 라우터(100)에서의 바인딩 업데이트 과정을 설명하기 위한 흐름도이다.
- <88> 모바일 노드(10)는 라우터(100)가 송신한 HoT 메시지와 CoT 메시지에 포함된 Home Keygen Token 및 Care-of Keygen Token을 이용하여 상기 수학식3에 따라 라우터(100)에 저장된 인증키 Kbm과 동일한 인증키를 생성한다. 모바일 노드(10)는 생성한 인증키 Kbm을 이용하여 모바일 노드(10)의 원격지 주소(CoA)를 포함하는 바인딩 업데이트(BU: Binding Update) 패킷을 송신한다. 이 때 바인딩 업데이트 패킷의 헤더에 설정된 소스 어드레스는 모바일 노드(10)의 홈 어드레스이고 목적지 어드레스는 CN1의 어드레스이다.

- <89> 라우터(100)는 제1 인터페이스(110)를 통해 바인딩 업데이트 패킷을 수신한다(제410 단계).
- <90> 제1 인터페이스(110)를 통해 바인딩 업데이트 패킷을 입력받은 패킷 감시부(120)는 입력된 패킷이 바인딩 업데이트 패킷임을 감지하여 제어부(130)로 패킷을 전달한다.
- <91> 제어부(130)는 인증테이블을 검색하여 CN1에 부여된 인증키 Kbm을 이용하여 바인딩 업데이트 패킷을 인증한 후, 바인딩 업데이트 패킷에 포함된 모바일 노드(10)의 원격지 어드레스를 모바일 노드(10)의 홈 어드레스와 함께 쌍으로 저장한다(제430 단계).
- <92> 도 9는 바인딩 캐쉬(141)의 일 예를 나타내는 도면이다. 도 9를 참조하면, 바인딩 캐쉬(141)는 각각의 상대방 노드별 바인딩 캐쉬(141a, 141b)을 구비하고, 각 상대방 노드별 바인딩 캐쉬는 각 상대방 노드와 통신을 하는 다수의 모바일 노드에 관한 바인딩 정보를 저장한다.
- <93> CN1의 바인딩 캐쉬(141a)에 모바일 노드(10)의 바인딩 정보를 MN1 엔트리에 저장한 후, 라우터(100)는 바인딩 업데이트가 완료되었음을 나타내는 바인딩 승인 메시지(Binding Acknowledgement Message)를 모바일 노드(10)에게 전송한다. 만약, 바인딩이 실패한 경우에는 바인딩 승인 메시지에 포함된 상태(Status) 필드에 바인딩이 실패했음을 나타내는 소정 값을 기록하여 전송한다. 바인딩이 실패한 경우에는 종래와 동일하게, 모바일 노드(10)와 CN1(60)은 홈 에이전트(30)를 경유하여 패킷을 인캡슐레이션 및 디캡슐레이션하여 상호 패킷을 교환한다.
- <94> 도 10은 바인딩 업데이트 완료 후, 모바일 노드(10)가 상대방 노드(MN1)로 전송한 패킷을 라우터(100)가 처리하는 과정을 설명하기 위한 흐름도이다.
- <95> 제1 인터페이스(110)를 통해 모바일 노드(10)가 송신한 패킷을 수신한다(제510 단계).

- <96> 제1 인터페이스(110)로부터 모바일 노드(10)가 송신한 패킷을 입력받은 패킷 감시부(120)는 입력된 패킷의 헤더를 검색하여, 패킷 헤더에 포함된 바인딩 정보를 추출하여 제어부(130)로 출력한다(제530 단계). 그리고 패킷 감시부(120)는 입력된 패킷을 패킷 변환부(150)로 출력한다.
- <97> 바인딩 정보는 패킷 헤더에 기록된 데이터 중, 소스 어드레스 영역에 기록된 모바일 노드(10)의 원격지 어드레스, 목적지 어드레스 영역에 기록된 MN1(60)의 어드레스 및 옵션 영역에 기록된 모바일 노드(10)의 홈 어드레스이다.
- <98> 제어부(130)는 바인딩 캐쉬(141)의 CN1의 바인딩 캐쉬(141a)를 검색하여 입력된 바인딩 정보, 즉 모바일 노드(10)의 원격지 어드레스 및 홈 어드레스가 CN1의 바인딩 캐쉬(141a)에 존재하는지 여부를 판단한다(제550 단계).
- <99> 모바일 노드(10)의 원격지 어드레스 및 홈 어드레스가 CN1의 바인딩 캐쉬(141a)에 존재하면, 제어부(130)는 패킷 변환부(150)를 제어하여 패킷 변환부(150)가 입력받은 패킷의 헤더의 소스 어드레스를 모바일 노드(10)의 원격지 어드레스에서 홈 어드레스로 변환하도록 패킷 변환부(150)를 제어한다.
- <100> 패킷 변환부(150)는 제어부(130)의 제어에 따라 패킷 감시부(120)로부터 입력받은 패킷의 헤더의 소스 어드레스를 모바일 노드(10)의 홈 어드레스로 변환한다(제560 단계).
- <101> 도 12는 패킷 변환부(150)가 패킷의 소스 어드레스를 변환하는 일 예를 나타내는 도면이다.

- <102>        왼쪽의 패킷 헤더는 변환 전 헤더로서, 소스 어드레스는 모바일 노드(10)의 원격지 어드레스가 기록되고 목적지 어드레스(Destination Address)는 CN1(60)의 어드레스가 기록되고, 옵션 영역에 모바일 노드(10)의 홈 어드레스가 기록 것이다.
- <103>        오른쪽 패킷 헤더는 변환된 후의 헤더로서, 소스 어드레스가 모바일 노드(10)의 홈 어드레스로 변환되었고, 옵션 영역이 제거되었다.
- <104>        패킷 변환부(150)는 헤더가 변환된 패킷을 제2 인터페이스(160)로 출력하고, 제2 인터페이스(160)는 CN1(60)으로 패킷을 전송한다(제570 단계). 한편, 제550 단계에서의 판단 결과, 제어부(130)에 입력된 바인딩 정보가 바인딩 캐쉬(141)에 존재하지 않으면, 제어부(130)의 제어에 따라 패킷 변환부(150)는 패킷의 홈 어드레스를 변환하지 않고 패킷을 출력하여, 해당 어드레스로 패킷이 전송되도록 한다.
- <105>        도 11은 데이터 저장부(140)내의 네이버 캐쉬(Neighbor Cashe)(145)의 일 예를 나타내는 도면이다. 도 11을 참조하면, 네이버 캐쉬(145)는 상대방 노드별 엔트리들로 구성된다. 각 엔트리는 각 상대방 노드의 어드레스, MAC(Medium Access Control) 어드레스 및 어드레스의 유효기간을 나타내는 라이프 타임 등의 데이터 필드를 포함한다.
- <106>        라우터(100)는 네이버 캐쉬(145)에 저장된 CN1(60)의 어드레스 및 MAC 어드레스에 따라 CN1(60)으로 변환된 패킷을 전송한다.
- <107>        CN1(60)은 소스 어드레스가 모바일 노드(10)의 홈 어드레스로 기록된 패킷을 수신하기 때문에 보안을 위한 인증, 바인딩 업데이트 및 패킷 변환 등의 모바일 IPv6의 기능을 수행할 수 없더라도 모바일 IPv6 기능을 가지는 모바일 노드로서 원격지 링크에 위치한 모바일 노드(10)가 송신한 패킷을 수신할 수 있다.

- <108> 도 13은 상대방 노드가 전송한 패킷을 수신하여 처리하는 과정을 설명하기 위한 흐름도이다.
- <109> 도 10에 도시한 바와 같은 과정에 의해 라우터(100)로부터 패킷을 전송받은 CN1(60)이 소스 어드레스를 모바일 노드(10)의 홈 어드레스로 한 패킷을 송신하고, CN1(60)이 송신한 패킷은 제2 인터페이스(160)를 통해 라우터(100)가 수신한다(제610 단계).
- <110> 제2 인터페이스(160)로부터 CN1(60)이 송신한 패킷을 입력받은 패킷 감시부(120)는 입력된 패킷의 헤더를 검색하여, 패킷 헤더에 기록된 목적지 어드레스를 추출하여 제어부(130)로 출력한다(제620 단계). 본 실시예에서 목적지 어드레스는 모바일 노드(10)의 홈 어드레스이다. 또한, 패킷 감시부(120)는 입력된 패킷을 패킷 변환부(150)로 출력한다.
- <111> 제어부(130)는 바인딩 캐쉬(141)의 CN1의 바인딩 캐쉬(141a)를 검색하여 입력받은 목적지 어드레스, 즉 모바일 노드(10)의 홈 어드레스가 모바일 노드(10)의 원격지 어드레스와 바인딩되어 미리 저장되어 있는지 여부를 판단한다(제630 단계).
- <112> 바인딩 캐쉬(141)에 모바일 노드(10)의 홈 어드레스가 모바일 노드(10)의 원격지 어드레스와 바인딩되어 있으면, 제어부(130)는 패킷 변환부(150)를 제어하여 패킷 변환부(150)가 입력받은 패킷의 헤더의 목적지 어드레스를 모바일 노드(10)의 원격지 어드레스로 변환하도록 패킷 변환부(150)를 제어한다.
- <113> 패킷 변환부(150)는 제어부(130)의 제어에 따라 패킷 감시부(120)로부터 입력받은 패킷의 헤더의 목적지 어드레스를 모바일 노드(10)의 홈 어드레스에서 원격지 어드레스로 변환한다(제640 단계).

- <114> 도 14는 패킷 변환부(150)가 패킷의 목적지 어드레스를 변환하는 일 예를 나타내는 도면이다. 왼쪽의 패킷 헤더는 변환 전 헤더로서, 목적지 어드레스 영역에는 모바일 노드(10)의 홈 어드레스가 기록되고 소스 어드레스 영역에는 CN1(60)의 어드레스가 기록된다.
- <115> 오른쪽 패킷 헤더는 변환된 후의 헤더로서, 목적지 어드레스가 모바일 노드(10)의 원격지 어드레스로 변환되었다. 그리고, 패킷의 원래 목적지 어드레스로 기록된 모바일 노드(10)의 홈 어드레스는 타입 2 라우팅 헤더(Type2 Routing Header)의 형태로 헤더에 저장된다.
- <116> 패킷 변환부(150)는 헤더가 변환된 패킷을 제1 인터페이스(110)로 출력하고, 제1 인터페이스(110)는 변환된 헤더의 목적지 주소로 기록된 모바일 노드(10)의 원격지 주소에 따라 모바일 노드(10)로 패킷을 전송한다(제650 단계).
- <117> 만약, 제630 단계에서의 판단 결과, 입력된 패킷의 목적지 어드레스가 소정의 원격지 어드레스와 바인딩되어 바인딩 캐쉬(141)에 미리 저장되어 있지 않으면, 제어부(130)는 패킷 변환부(150)를 제어하여 목적지 어드레스를 변환하지 않도록 한다. 패킷 변환부(150)는 입력받은 패킷을 그대로 제1 인터페이스(110)로 출력하고, 제1 인터페이스(110)는 패킷의 목적지 어드레스에 따라 패킷을 전송한다(제660 단계).
- <118> 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장 장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드로 저장되고 실행될 수 있다.

## 【발명의 효과】

<119>       이상에서 설명한 바와 같이, 본 발명에 따른 모바일 노드와의 접속을 제공하는 라우터 및 그 라우팅 방법은, 모바일 노드와의 통신을 위해 필요한 모바일 기능을 구비하지 아니한 상대방 노드와 모바일 노드간의 직접 통신을 가능하게 하는 효과를 제공한다.



**【특허청구범위】****【청구항 1】**

원격지 링크에 접속한 모바일 노드와 상대방 노드간에 패킷을 전달하는 라우터에 있어서,

적어도 인증키 생성 토큰을 생성하기 위한 데이터를 저장하는 데이터 저장부;

패킷을 수신하거나 송신할 패킷의 헤더에 기록된 목적지 어드레스로 패킷을 송신하는 제1 인터페이스;

상기 제1 인터페이스로부터의 출력된 패킷이 상기 모바일 노드의 인증을 요청하는 인증요청패킷이면 상기 인증요청패킷을 출력하는 패킷 감시부;

상기 패킷 감시부의 출력인 상기 입력 패킷을 입력받아, 상기 데이터 저장부에 저장된 인증키 생성 토큰을 생성하기 위한 데이터를 참조하여 인증키 생성 토큰을 생성하고, 상기 인증키 생성 토큰을 이용하여 인증키를 생성한 후, 상기 인증키 생성 토큰 및 상기 인증키를 상기 데이터 저장부에 저장하고, 상기 인증키 생성 토큰을 상기 제1 인터페이스로 출력하는 제어부를 포함하고,

상기 제1 인터페이스는 상기 인증키 생성 토큰을 입력받아 상기 모바일 노드로 전송하는 것을 특징으로 하는 라우터.

**【청구항 2】**

제1 항에 있어서,

상기 패킷 감시부는 상기 제1 인터페이스가 수신하여 출력한 패킷이 상기 모바일 노드가 상기 인증키 생성 토큰에 따라 생성한 인증키를 이용하여 암호화한 바인딩 업데이트 패킷이면 상기 바인딩 업데이트 패킷을 상기 제어부로 출력하고,

상기 제어부는 상기 바인딩 업데이트 패킷에 포함된, 상기 모바일 노드의 홈 어드레스와 상기 원격지 링크에서 부여받은 원격지 어드레스를 포함하는 바인딩 정보를 상기 데이터 저장부에 저장된 상기 인증키를 이용하여 추출하여 상기 데이터 저장부에 저장하는 것을 특징으로 하는 라우터.

### 【청구항 3】

제2 항에 있어서, 상기 라우터는

상기 패킷 감시부로부터 출력된 패킷을 입력받아, 상기 제어부의 제어에 따라 상기 모바일 단말기의 원격지 주소로 설정된 소스 어드레스를 상기 홈 어드레스로 패킷을 변환하여 출력하는 패킷 변환부; 및

상기 패킷 변환부에서 출력된 패킷을 입력받아, 상기 패킷의 헤더에 기록된 상기 상대방 노드의 어드레스에 따라 상기 패킷을 상기 상대방 노드로 전송하는 제2 인터페이스를 더 포함하고,

상기 패킷 감시부는 상기 제1 인터페이스가 수신하여 출력한 패킷의 헤더를 검색하여, 상기 패킷 헤더에 포함된 바인딩 정보를 상기 제어부로 출력하고, 상기 패킷 변환부로 수신한 패킷을 출력하고,

상기 제어부는 상기 데이터 저장부를 검색하여 상기 바인딩 정보가 상기 데이터 저장부에 존재하면, 소스 어드레스가 상기 홈 어드레스로 변환된 패킷을 출력하도록 상기 패킷 변환부를 제어하는 것을 특징으로 하는 라우터.

【청구항 4】

제3 항에 있어서,

상기 제어부는 상기 데이터 저장부를 검색하여 상기 바인딩 정보가 상기 데이터 저장부에 존재하지 않으면, 상기 패킷에 포함된 소스 어드레스를 변환하지 않고 상기 패킷을 통과시키도록 상기 패킷 변환부를 제어하는 것을 특징으로 하는 라우터.

【청구항 5】

제3 항에 있어서,

상기 제2 인터페이스는 상기 상대방 노드가 송신한 패킷을 수신하여 상기 패킷 감시부로 출력하고,

상기 패킷 감시부는, 상기 제2 인터페이스로부터 입력받은 패킷의 헤더에 기록된 목적지 어드레스를 상기 제어부로 출력하고, 상기 패킷 변화부로 입력받은 패킷을 출력하고,

상기 제어부는 상기 데이터 저장부를 검색하여 상기 목적지 어드레스가 상기 모바일 노드의 홈 어드레스이고 상기 홈 어드레스가 상기 모바일 노드의 원격지 어드레스와 바인딩되어 있으면, 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하도록 상기 패킷 변환부를 제어하고,

상기 패킷 변환부는 상기 제어부의 제어에 따라 상기 상대방 노드가 송신한 패킷의 헤더에 기록된 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하여 상기 제1 인터페이스로 출력하는 것을 특징으로 하는 라우터.

**【청구항 6】**

원격지 링크에 접속한 모바일 노드와 상대방 노드간에 패킷을 전달하는 라우팅 방법에 있어서,

(a) 상기 모바일 노드로부터 송신된 패킷이 상기 모바일 노드의 인증을 요청하는 인증요청패킷인지 여부를 감시하는 단계;

(b) 상기 모바일 노드로부터 송신된 패킷이 상기 모바일 노드의 인증을 요청하는 인증요청패킷이면, 미리 저장된 인증키 생성 토큰을 생성하기 위한 데이터를 참조하여 인증키 생성 토큰을 생성하는 단계;

(c) 생성된 인증키 생성 토큰에 따라 생성한 인증키 및 상기 인증키 생성 토큰을 저장하는 단계; 및

(d) 상기 모바일 노드로 상기 인증키 생성 토큰을 송신하는 단계를 포함하는 것을 특징으로 하는 라우팅 방법.

**【청구항 7】**

제6 항에 있어서,

(e) 상기 모바일 노드가 상기 인증키 생성 토큰에 따라 생성한 인증키를 이용하여 인증한 바인딩 업데이트 패킷을 수신하는 단계; 및

(f) 상기 바인딩 업데이트 패킷에 포함된, 상기 모바일 노드의 홈 어드레스와 상기 원격지 링크에서 부여받은 원격지 어드레스를 포함하는 바인딩 정보를 미리 저장한 상기 인증키를 이용하여 추출한 후 저장하는 단계를 더 포함하는 것을 특징으로 하는 라우팅 방법.

**【청구항 8】**

제7 항에 있어서,

(g) 상기 모바일 노드가 송신한 패킷으로서 바인딩 정보 및 데이터를 포함하는 패킷을 수신하는 단계;

(h) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하는지 여부를 검색하는 단계;

(i) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하면, 상기 원격지 주소로 설정된 소스 어드레스를 상기 홈 어드레스로 변환하는 단계; 및

(j) 상기 소스 어드레스가 변환된 패킷을 상기 상대방 노드로 전송하는 단계를 더 포함하는 것을 특징으로 하는 라우팅 방법.

**【청구항 9】**

제8 항에 있어서,

(k) 저장된 다수의 바인딩 정보 중 상기 모바일 노드가 송신한 패킷에 포함된 바인딩 정보와 일치하는 바인딩 정보가 존재하지 않으면, 상기 패킷에 포함된 소스 어드레스를 변환하지 않고 패킷을 상기 상대방 노드로 전송하는 단계를 더 포함하는 것을 특징으로 하는 라우팅 방법.

**【청구항 10】**

제8 항에 있어서,

(1) 상기 상대방 노드가 송신한 패킷의 헤더에 목적지 어드레스로 기록된 상기 모바일 노드의 홈 어드레스를 추출하는 단계;

(m) 저장된 다수의 바인딩 정보를 검색하여 상기 모바일 노드의 홈 어드레스와 바인딩된 상기 모바일 노드의 원격지 어드레스를 추출하는 단계;

(n) 상기 상대방 노드가 송신한 패킷의 헤더의 목적지 어드레스를 상기 모바일 노드의 원격지 어드레스로 변환하는 단계; 및

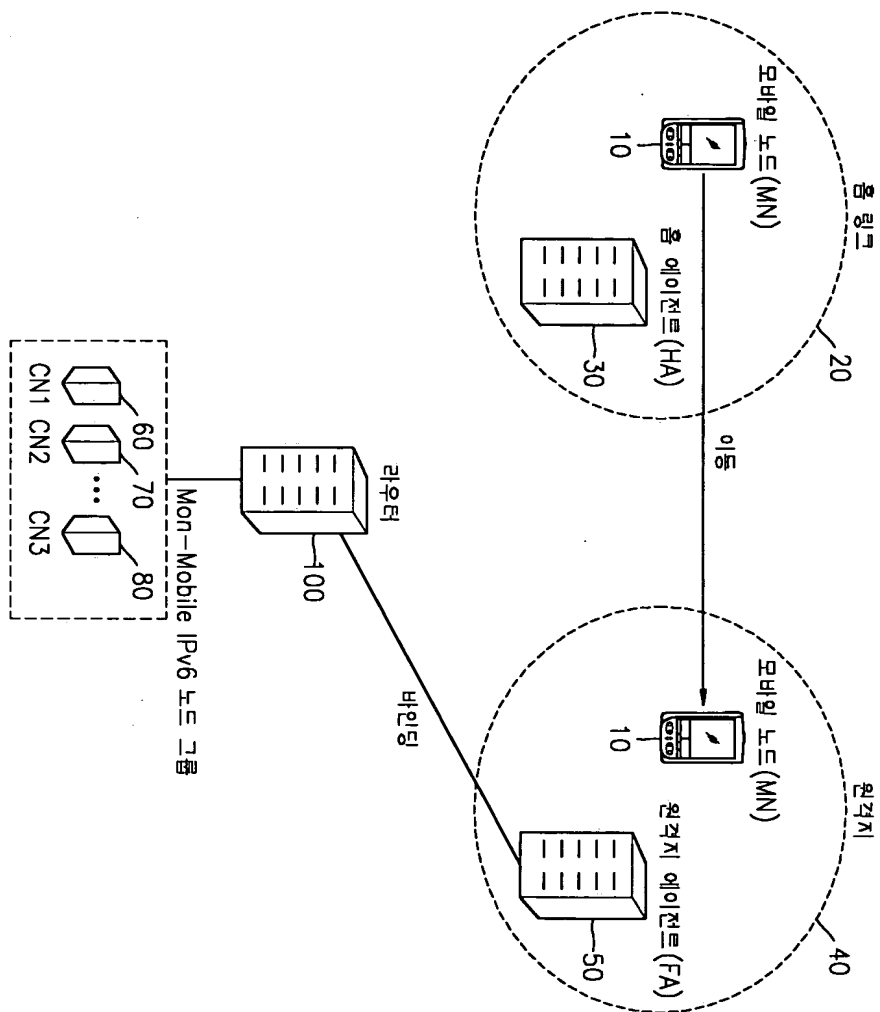
(o) 상기 상대방 노드의 원격지 어드레스에 따라 상기 상대방 노드가 송신한 패킷을 상기 모바일 노드로 송신하는 단계를 더 포함하는 것을 특징으로 하는 라우팅 방법.

**【청구항 11】**

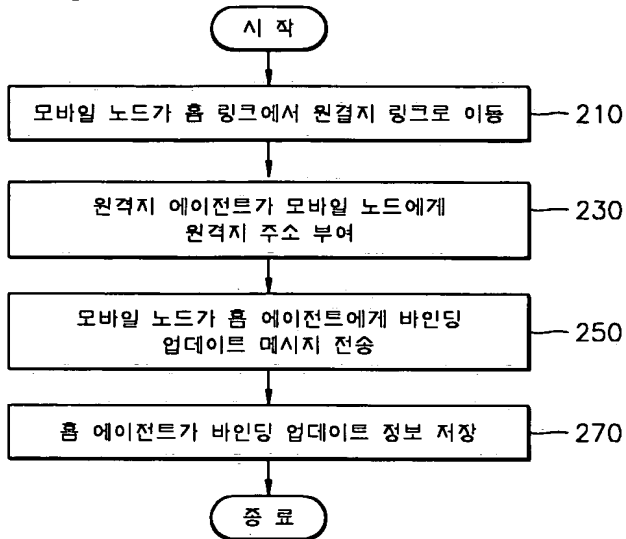
제6 항 내지 제10 항 중 어느 한 항에 기재된 방법을 실현하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

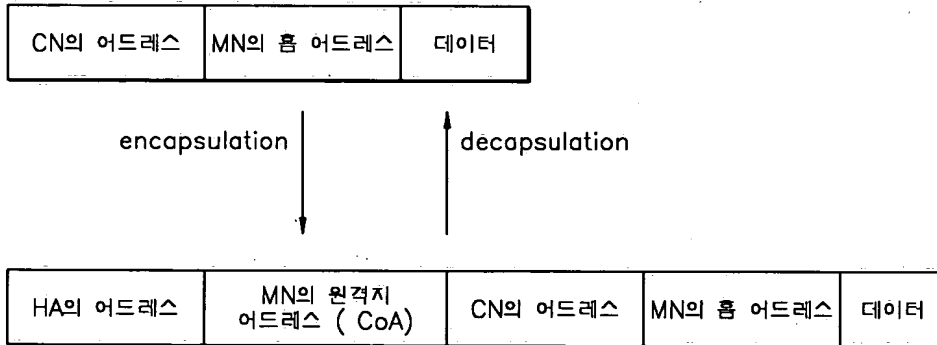
【도 1】



【도 2】

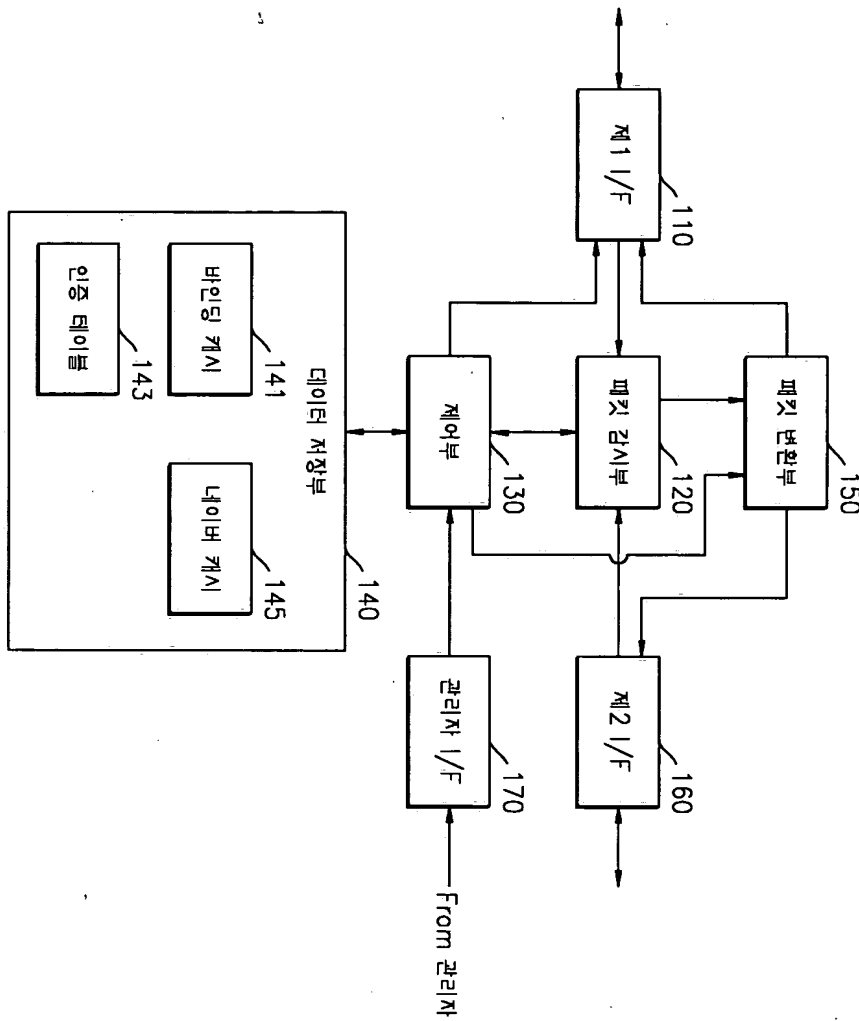


【도 3】

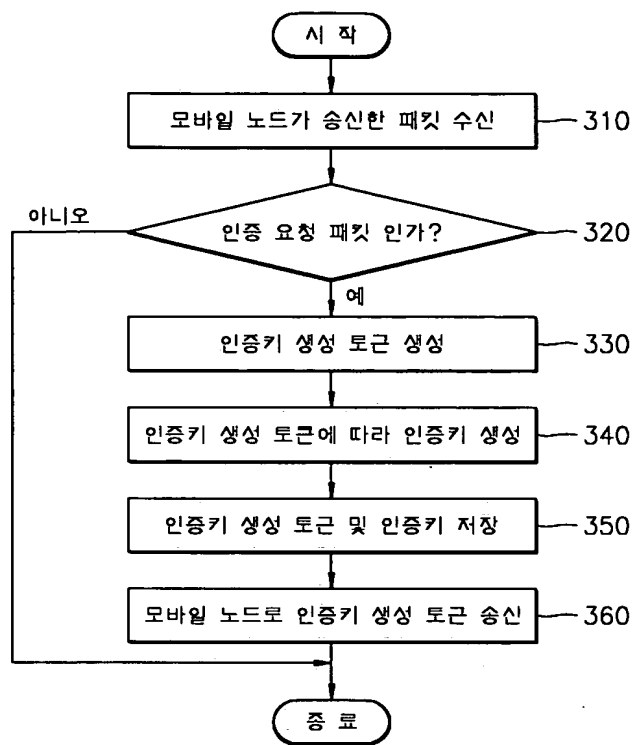




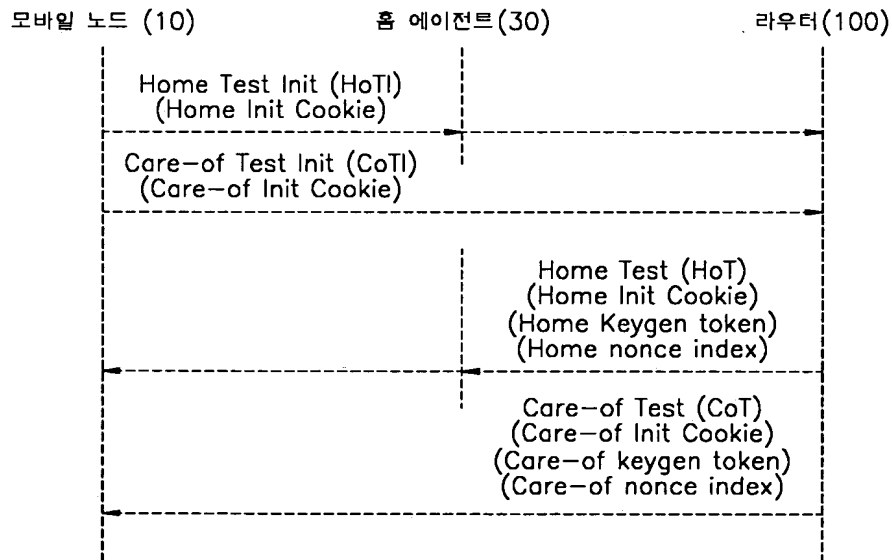
【도 4】



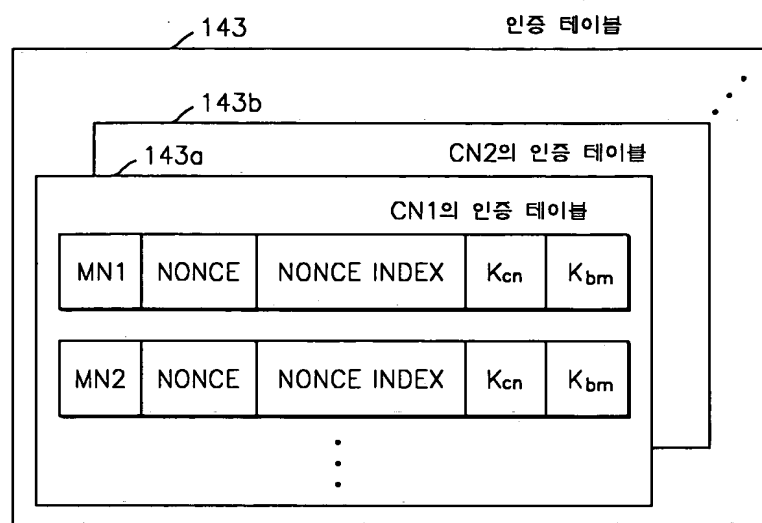
【도 5】



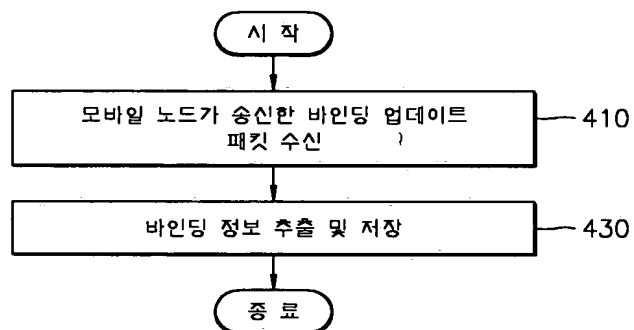
【도 6】



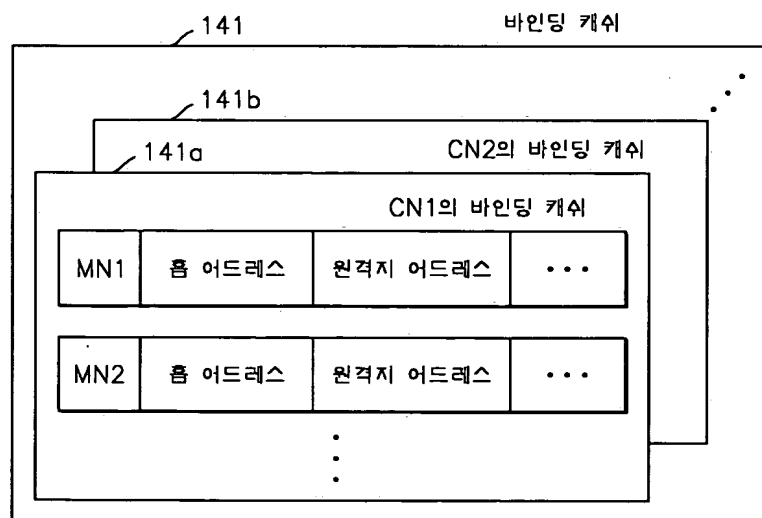
【도 7】



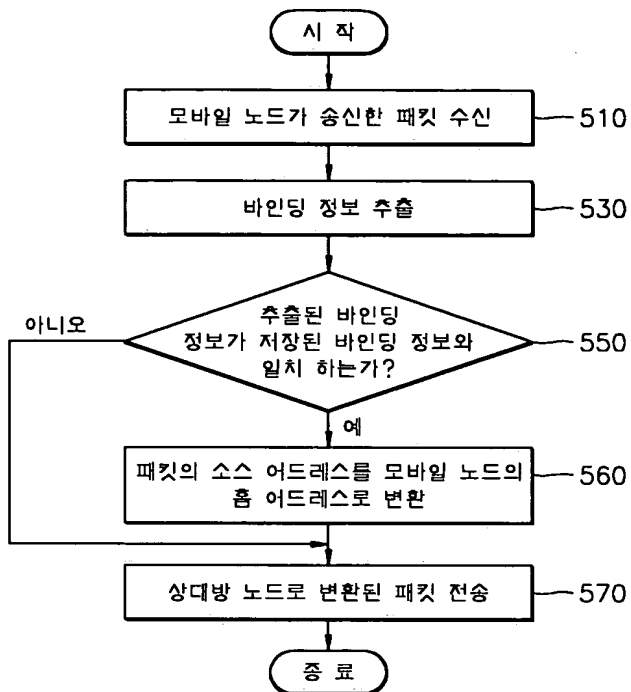
【도 8】



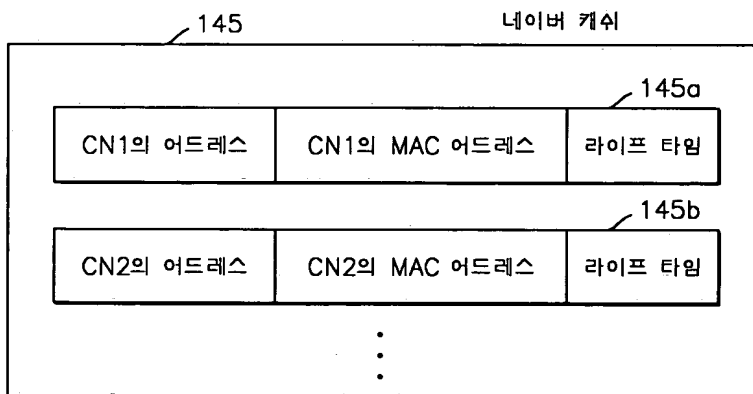
【도 9】



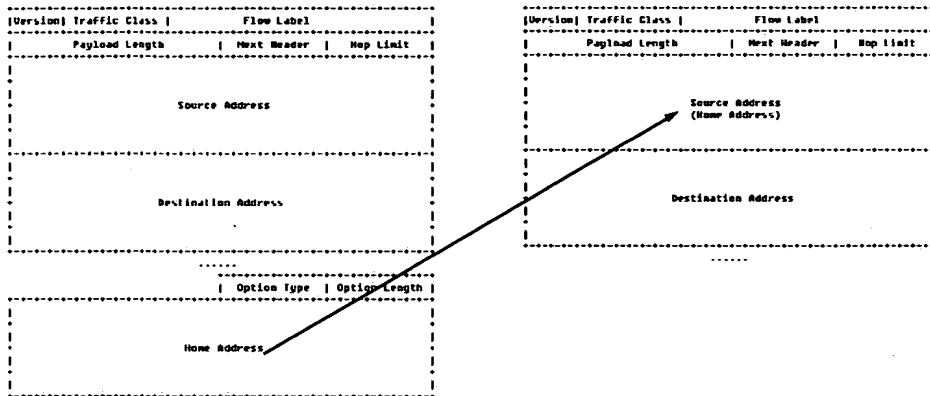
【도 10】



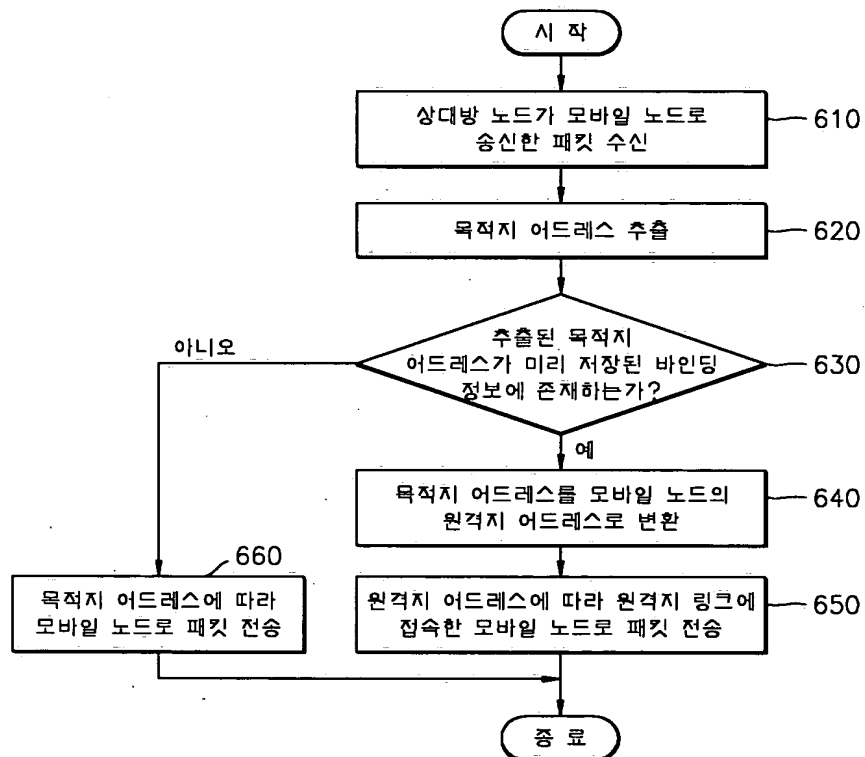
【도 11】



【도 12】



【도 13】



【도 14】

